FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

DRR Imaging and Indexing Services

VASTEC, Inc.

(RECVR-15-C-0693)

Date Approved by Chief Privacy Officer (CPO)/Designee: 9/19/2016

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the federal government and was established by Congress in 1933. Its mission is to maintain the stability and public confidence in the nation's financial system by insuring bank deposits, examining and supervising financial institutions, and managing failed bank receiverships. In its receivership capacity, FDIC is charged with liquidating assets efficiently, maximizing recoveries, and managing claims and litigation demands.

To ensure a seamless transition for customers prior to a bank failure, the FDIC often pursues arrangements for a healthy institution to assume the deposits, loans, and other assets of the failing bank. The resulting closing transaction can often necessitate that the FDIC retain, manage, and market some of the assets (loans, properties, and interests) to achieve the best possible return for the receivership. In its Receivership capacity, the FDIC seeks to contract with a national firm with a proven track record of working with firms or other government agencies engaged in the secondary loan sale markets to manage the imaging, indexing, and delivery of documents for an FDIC structured sale.

In addition to marketing efforts, the FDIC must also discharge its statutory duties and maximize recoveries from claims and lawsuits relating to the professional and criminal liability of individuals related to failed financial institutions (FIs). Critical to the legal support of these FDIC investigations are several administrative services including electronic imaging, copying, Bates numbering, indexing, and converting bank records into searchable digital files. The FDIC has contracted with VASTEC, Inc. (VASTEC) to provide such services to the FDIC's Division of Resolutions and Receiverships (DRR) at the FDIC's Field Operations Branch in Dallas, TX. In conjunction with providing those services, VASTEC may obtain data records from failed FIs that include attorney work products, board minutes, floor plans, loan files. Additionally, VASTEC may obtain CDs which contain borrower personally identifiable information (PII) as specified in the responses to questions 3 and 5 below.

SECTION II – DATA TYPE, SOURCES, AND USE

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

FDIC DRR personnel in Dallas, TX physically deliver data records to the on-site VASTEC office for imaging and indexing services. The data records are collected from failed FIs and may include attorney work products, board minutes, floor plans, loan files, and CDs, DVDs and other electronic media which may contain PII such as full names, date of birth, place of birth, SSN, employment information, mother's maiden name, home addresses, phone numbers, email addresses, employee identification numbers, financial information, driver's license identification numbers, vehicle identifiers, legal documents and/or investigative reports. FDIC data is not transferred to VASTEC's

corporate network, as VASTEC's scanning and indexing services team uses an isolated local network which is not connected to the internet or any other external networks. Scanned records are temporarily uploaded to an assigned hard drive dedicated for FDIC data, where they are converted and burned to an encrypted DVD. The original records are physically returned to the on-site FDIC DRR representative who initially delivered them. Records pending imaging and indexing remain on-site, and are secured in an FDIC-approved cabinet, in a locked office. All stored data is encrypted utilizing BitLocker password-protected volumes; all FDIC data stored on the dedicated drive is also encrypted utilizing SecureZip for Windows.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

In its receivership capacity, FDIC is charged with liquidating assets efficiently, maximizing recoveries, and managing claims and litigation demands. To help satisfy these responsibilities, the FDIC/DRR Investigations Group, in coordination with the Legal Division Professional Liability and Financial Crimes Group, conducts investigations to determine the causes of the institution's failure and, if necessary, takes legal action against "Persons-of-Interest" (POIs) who may have committed crimes or otherwise breached their duties to the failed institution. In this regard, the PII identified above will be used by FDIC/DRR Investigations, Legal, and FDIC Outside Counsel to support ongoing investigations involving professional liability claims, criminal restitutions, litigation, and as needed, the internal department needs of FDIC/DRR Investigations. As part of these investigations, the electronic images also may be provided securely to Opposing Counsel by FDIC as required. . After receiving the original data records, and the work product, DRR updates their records and ships everything to Iron Mountain in case it is needed in the future.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above? *(This is not intended to be an all-inclusive list. Specify other categories of PII, as needed.)*:

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☒	☐
Vehicle Identifiers (e.g., license plates)	☒	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐

Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☐	☒
Investigation Report or Database	☒	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: _____)	☐	☒

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs: SSNs may be included in the information provided by the failed FIs. In order to satisfy the responsibilities of liquidating assets efficiently, maximizing recoveries, and managing claims and litigation demands, SSNs may be included in the information that VASTEC is tasked with imaging and indexing.

b) Provide the legal authority which permits the collection of SSNs.

12 U.S.C. § 1820, et. seq.

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: No

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☒
5,001 – 7,500 ☐	7,501 – 10,000 ☐	10,001 – 50,000 ☐	50,001 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[1]: N/A

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[2] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
FDIC DRR	Data records are physically provided to VASTEC personnel by the contract Technical Monitor and/or other assigned FDIC DRR	☒ Yes ☐ No

[1] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[2] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

	representative, typically in an Iron Mountain box. The data records are collected from failed FIs and may include attorney work products, board minutes, floor plans, loan files, and CDs, DVDs and other electronic media which may contain PII such as full names, date of birth, place of birth, SSN, employment information, mother's maiden name, home addresses, phone numbers, email addresses, employee identification numbers, financial information, driver's license identification numbers, vehicle identifiers, legal documents and/or investigative reports.	

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?
Yes, data can be retrieved using a personal identifier (VASTEC indexes data records by loan ID numbers).

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name. 30-64-0013, *Insured Financial Institution Liquidation Records.*

This completes the PTA.

- Do <u>not</u> complete the rest of the form, if the service provider is <u>not</u> processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 thru 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that the Outsourced Service Provider will share or provide PII data to as part of the outsourced service. ***(Check "No" or "Yes" for each category. For each category checked "Yes," specify who will have access to, be provided with, or maintain the PII, what PII elements will be accessed/shared/maintained by them, how the access or sharing will occur, and the purpose and use of this PII.)***

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	VASTEC receives physical data records from the contract Technical Monitor and/or an assigned FDIC DRR representative via job box (typically an Iron Mountain box). These physical data records are imaged and stored temporarily on an on-site hard drive dedicated for FDIC data, and burned onto encrypted DVDs. All data is stored on a BitLocker-encrypted password-protected drive, and also secured utilizing SecureZIP for Windows. Only two VASTEC employees, the Program Manager and Document Imaging Associate, will have access to the data records that contain PII, such as full names, date of birth, place of birth, SSN, employment information, mother's maiden name, home addresses, phone numbers, email addresses, employee identification numbers, financial information, driver's license identification numbers, vehicle identifiers, legal documents and/or investigative reports. The office is secured at the end of the business day, and any remaining data records are secured inside an FDIC-approved cabinet.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	VASTEC returns all original data records and encrypted DVDs back to the contract Technical Monitor and/or appointed FDIC DRR representative who physically retrieves the job box. The FDIC DRR representative will then return original paper records with the encrypted DVDs and the updated Chain of Custody form to their source which is typically back to FDIC physical storage with Iron Mountain. The passwords to access data on the encrypted DVDs are sent to the OM via the FDIC Secure Email Service. Anyone that requests the encrypted DVDs from storage must contact the TM for the password. The encrypted DVD is then used to review the box contents electronically. Authorized FDIC staff, such as Legal Division staff and FDIC Office of Inspector General (OIG) staff, may have the imaged data shared with them on a "need to know" basis in support of investigations involving professional liability claims, criminal restitutions, and litigation.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers,	☐	☒	N/A

etc.)			
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☒	☐	Authorized FDIC staff (e.g., FDIC/DRR or Legal staff) may securely provide the electronic documents/digital images, which may contain some or all of the PII identified above, to Opposing Counsel by FDIC, as required for ongoing investigations involving professional liability claims, criminal restitutions, and litigation.
10e. Federal, State, and/or Local Agencies	☐	☒	N/A
10f. Other	☐	☒	N/A

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☒	☐
FDIC Confidentiality Agreement (Individual)	☒	☐
Non-Disclosure Agreement (NDA)	☒	☐
Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: _____)	☐	☒
If you answered NO to any item above, please provide additional information if available: VASTEC is an outsourced service provider/vendor and is not subject to MOUs or ISAs.		

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information. ***(Explain why individuals are not able to opt out (either for specific data elements or specific uses of their data.):***

☐ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. ***(Explain how individuals may decline or consent to the use of their information.):***

☒ Not applicable. Information is not collected directly from individuals.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☐ Yes *(If yes, check applicable box(es) below.)*
- ☐ Link to FDIC Privacy Policy
- ☐ FDIC Privacy Act Statement
- ☐ Contractor Privacy Policy or Statement
- ☐ No Privacy Policy has been posted

☒ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care. *[Provide the name of the Outsourced Service Provider and check all applicable box(es).]*

☒ VASTEC has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☒ YES

☒ The FDIC conducts background investigations (BIs) on key VASTEC personnel and other applicable personnel prior to their beginning work on the contract.

☒ The VASTEC is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsource Service

Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

☐ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form.***

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date? *[Check all applicable box(es) and insert the appropriate response and System/Project name.]*

☐ Data is collected directly from individuals and/or from the failed financial institutions. As such, the FDIC and its vendors rely on the individuals and/or financial institutions to provide accurate data.

☒ The vendor/contractor works with FDIC to verify the integrity of the data before inputting it into the system or using it to support the project.

☒ As necessary, a Project Manager of the DRR Imaging and Indexing Services checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☐ Other

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider. (*Check all applicable box(es) and insert the name of the Outsourced Information Service Provider and title of the firm's senior management official.*)

☒ Within FDIC, VASTEC's Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated the Project Manager to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection.

Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

VASTEC will only receive physical data records from the contract Technical Monitor or FDIC DRR on-site representative. These data records will be stored on-site at the FDIC's Dallas location. Scanned data records will be temporarily stored on VASTEC's dedicated network drive and secured utilizing BitLocker disk volume encryption. All FDIC data temporarily stored on that drive is encrypted utilizing SecureZip for Windows. In the event data records have not been imaged, they will remain on-site and secured in an FDIC approved cabinet, and the physical office will be locked.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

VASTEC's retention policy is three (3) years following final payment under this contract, or for any longer period required by statute or another clause in their contract. VASTEC has a 180 day retention policy, after 180 days files are destroyed giving FDIC advanced authorization of certified approved destruction. Electronic files are wiped using File Shredder v2.5 and the DoD 5220-22.M standard with 3-pass overwrite.